PTO/SB/21 (02-04)
Approved for use through 07/31/2006. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Application Number	10/799,215
Filing Date	3/11/2004
First Named Inventor	Kazuomi Olshi
Art Unit	2131
Examiner Name	unknown
Attorney Docket Number	CFA00096US

Total Number of Pages in This Submission: 40

ENCLOSURES *(Check all that apply)*

- ☐ Fee Transmittal Form
  - ☐ Fee Attached
- ☐ Amendment/Reply
  - ☐ After Final
  - ☐ Affidavits/declaration(s)
- ☐ Extension of Time Request
- ☐ Express Abandonment Request
- ☐ Information Disclosure Statement
- ☑ Certified Copy of Priority Document(s)
- ☐ Response to Missing Parts/ Incomplete Application
  - ☐ Response to Missing Parts under 37 CFR 1.52 or 1.53
- ☐ Drawing(s)
- ☐ Licensing-related Papers
- ☐ Petition
- ☐ Petition to Convert to a Provisional Application
- ☐ Power of Attorney, Revocation Change of Correspondence Address
- ☐ Terminal Disclaimer
- ☐ Request for Refund
- ☐ CD, Number of CD(s) _____
- ☐ After Allowance communication to Technology Center (TC)
- ☐ Appeal Communication to Board of Appeals and Interferences
- ☐ Appeal Communication to TC **(Appeal Notice, Brief, Reply Brief)**
- ☐ Proprietary Information
- ☐ Status Letter
- ☐ Other Enclosure(s) (please Identify below):

Remarks

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm or Individual name	Canon U.S.A., Inc. IP Department Fidel Nwamu
Signature	Fidel Nwamu
Date	6/23/04

CERTIFICATE OF TRANSMISSION/MAILING

I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below.

Typed or printed name	Fidel Nwamu		
Signature	Fidel Nwamu	Date	6/23/04

CFA00096
US

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００３年　５月２９日

出願番号
Application Number: 特願２００３－１５２８３４

[ST. 10/C]: [ＪＰ２００３－１５２８３４]

出願人
Applicant(s): キヤノン株式会社

２００４年　６月１４日

特許庁長官
Commissioner,
Japan Patent Office 今井康夫

出証番号　出証特２００４－３０５０９４８

【書類名】　特許願
【整理番号】　254654
【提出日】　平成15年 5月29日
【あて先】　特許庁長官　太田　信一郎　殿
【国際特許分類】　H04L 12/40
【発明の名称】　特定アドレス使用制限装置
【請求項の数】　7
【発明者】
【住所又は居所】　東京都大田区下丸子３丁目３０番２号キヤノン株式会社内
【氏名】　大石　和臣
【特許出願人】
【識別番号】　000001007
【住所又は居所】　東京都大田区下丸子３丁目３０番２号
【氏名又は名称】　キヤノン株式会社
【代表者】　御手洗　冨士夫
【代理人】
【識別番号】　100090538
【住所又は居所】　東京都大田区下丸子３丁目３０番２号キヤノン株式会社内
【弁理士】
【氏名又は名称】　西山　恵三
【電話番号】　03-3758-2111

【選任した代理人】

【識別番号】　100096965

【住所又は居所】　東京都大田区下丸子３丁目３０番２号キヤノン株式会社内

【弁理士】

【氏名又は名称】　内尾　裕一

【電話番号】　03-3758-2111

【手数料の表示】

【予納台帳番号】　011224

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9908388

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　特定アドレス使用制限装置

【特許請求の範囲】

【請求項１】　他の装置が装置固有の識別子から特定方法で生成したネットワークアドレスの使用を試みていることを検出する検出手段と、

前記試みを検出すると、前記ネットワークアドレスの使用制限を通知する手段とを有することを特徴とする特定アドレス使用制限装置。

【請求項２】　前記ネットワークアドレスは、Internet Protocol Version 6（ＩＰｖ６）のネットワークアドレスであり、前記装置固有の識別子からネットワークアドレスを生成する特定方法は、ＩＥＥＥ　ＥＵＩ－６４形式のインターフェイスＩＤを用いてネットワークアドレスを生成する方法であり、前記通知手段は、ＩＰｖ６のNeighbor Discovery Protocolのa multicast Neighbor Advertisementを送信する手段であることを特徴とする前記請求項１記載の特定アドレス使用制限装置。

【請求項３】　他の装置が、装置固有の識別子から特定方法で生成したネットワークアドレスを含むデータを送信したことを検出する検出手段と、

前記送信を検出すると、特定ネットワークアドレスを含むデータの転送を中止する手段とを有することを特徴とする外部ネットワークとの中継を行なう特定アドレス使用制限装置。

【請求項４】　前記ネットワークアドレスは、Internet Protocol Version 6（ＩＰｖ６）のネットワークアドレスであり、前記装置固有の識別子からネットワークアドレスを生成する特定方法は、ＩＥＥＥ　ＥＵＩ－６４形式のインターフェイスＩＤを用いてネットワークアドレスを生成する方法であり、前記転送中止手段は、ＩＰｖ６のグローバルアドレスを用いたパケットをネットワーク外部に転送しない手段であることを特徴とする前記請求項３記載の特定アドレス使用制限装置。

【請求項５】　他の装置が装置固有の識別子から特定方法で生成したネットワークアドレスの使用を試みていることを検出し、

前記試みを検出すると、前記ネットワークアドレスの使用制限を通知する手段

とを有することを特徴とする特定アドレス使用制限方法。

【請求項６】　他の装置が、装置固有の識別子から特定方法で生成したネットワークアドレスを含むデータを送信したことを検出し、

前記送信を検出すると、特定ネットワークアドレスを含むデータの転送を中止する手段とを有することを特徴とする外部ネットワークとの中継方法。

【請求項７】　請求項５又は６の方法を実行するプログラム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、特定アドレスの使用を制限する装置に関する。

【０００２】

【従来の技術】

ＩＰｖ６に対応するパーソナル・コンピュータやワークステーションでは、ネットワークとの接続のインターフェイスには通常はイーサネット（Ｒ）が用いられ、それが持つＩＥＥＥ　ｉｄｅｎｔｉｆｉｅｒ（MAC address）を元にしてＩＰｖ６アドレスが生成される。この方法によって生成されたアドレスをＩＥＥＥＥＵＩ－６４形式のＩＰｖ６アドレスと呼ぶ。

【０００３】

ＩＰｖ６アドレスには、後述するようにリンクローカルアドレス、サイトローカルアドレスと（集約可能）グローバルアドレスの３種類が存在する。

【０００４】

それらの詳細や構成方法などのアドレス体系は、RFC 2373 ‘‘IPVersion 6 Addresssing Architecture、’’ ‘‘ RFC 2374 ‘‘An IPv6 Aggregatabale Global Unicast Address Format、’’ RFC 2375 ’’ IPv6 Multicast Address Assignment、’’ RFC 2450 ’’ Proposed TLA and NLA Assignment Rule、’’ RFC2461 ’’ Neighbor Discovery for IP Version 6 (IPv6)、’’ RFC 2462 ’’ IPv6 Stateless Address Autoconfiguration、’’ 等に記述されている。

【０００５】

ところで、ＩＥＥＥ　ＥＵＩ－６４形式のＩＰｖ６アドレスのように、ＩＥＥ

Ｅ　ｉｄｅｎｔｉｆｉｅｒ　（MAC address）等のハードウェアに１対１に対応する情報を固定的に用いて生成されたアドレスを使うと、それが装置もしくはその装置のユーザと１対１に対応する情報とみなされ、そのアドレスを使う通信をモニターされることによりプライバシが侵害される恐れが強い。

【０００６】

この課題に対しては、ランダムなＩＰｖ６アドレス（正確にはinterface ID）を生成する方法が、RFC3041 ’’ Privacy Extensions for Stateless Address Autoconfiguration in IPv6,’’ 等において提案されている。生成したランダムな値が既に使われている場合には、それを検出し、別のランダムな値を計算／生成し、ユニークなランダムな値を定めるプロトコル（の拡張）も記述されている。このランダムなＩＰｖ６アドレスは、ｔｅｍｐｏｒａｒｙ　ａｄｄｒｅｓｓあるいは匿名アドレスと呼ばれる。

【０００７】

【発明が解決しようとする課題】

しかし、全ての装置が匿名アドレスを常に使うとは限らない。ＩＥＥＥ　ＥＵＩ－６４形式のアドレスを使うように初期設定されている装置も存在すると考えられ、その装置がそのアドレスを継続使用するとプライバシが侵害される可能性がある。

【０００８】

【課題を解決するための手段】

上記課題を解決するために、本出願に関わる発明は、ローカルなネットワークに設けた特定アドレス使用制限装置が、ネットワーク上の他の装置がＩＥＥＥ　ＥＵＩ－６４形式のアドレスの使用を試みるか否かを判断し、前記他の装置がＩＥＥＥ　ＥＵＩ－６４形式のアドレス使用を試みる場合は、そのアドレスが既に使用されている旨のメッセージを送る手段を有する。

【０００９】

本手段により、ネットワーク上の装置がＩＥＥＥ　ＥＵＩ－６４形式のアドレスを使用することを防ぐことができるので、ＩＥＥＥ　ＥＵＩ－６４形式のアドレスを使用した通信をモニターされてプライバシが侵害される可能性を無くすこ

とができる。

【００１０】

上記課題を解決するために、本出願の他の発明では、ローカルなネットワークにおけるｄｅｆａｕｌｔ　ｇａｔｅｗａｙが特定アドレス使用制限装置を兼ねる。前記制限装置は、ネットワーク上の他の装置がＩＥＥＥ　ＥＵＩ－６４形式のアドレスを含むデータを送信するか否かを判断し、前記他の装置がＩＥＥＥ　ＥＵＩ－６４形式のアドレスを含むデータを送信する場合は、そのアドレスを記録し、そのアドレスを含むデータをネットワーク外部へ転送しないように処理する制御手段を有する。

【００１１】

本手段により、ネットワーク上の他の装置がＩＥＥＥ　ＥＵＩ－６４形式のアドレスを使用してネットワーク外部と通信することを防ぐことができるので、ＩＥＥＥ　ＥＵＩ－６４形式のアドレスを使用した通信をモニターされてプライバシが侵害される可能性を無くすことができる。

【００１２】

【発明の実施の形態】

（第１の実施の形態）

本実施の形態では、ホストがイーサネット（Ｒ）のＬＡＮ経由でインターネットと接続する場合を説明する。最初に現状を説明し、その後に本発明の実施の形態を説明する。

【００１３】

図２は、本発明が適用される接続環境（ホストがイーサネット（Ｒ）のＬＡＮ経由でインターネットと接続する環境）を模式的に示したものである。

【００１４】

図２は、ＬＡＮに接続されたホスト２０４、２０５、２０６がｇａｔｅｗａｙ２０２経由でインターネット２０１にアクセスする環境を示す。本実施の形態では、各ホストはリンク２０７で接続するものとし、具体的にはイーサネット（Ｒ）であるとする。２０８もリンクである。リンクとは、それに接続された装置がそれを介して通信することができる設備もしくはメディアであり、ＩＰ層の下側

に接する。リンクにはイーサネット（Ｒ）の他に、ＰＰＰリンク、Ｘ．２５、フレームリレー、ＡＴＭネットワークがある。リンクに接続されたＩＰｖ６装置をノードと呼ぶ。２０３はＤＨＣＰサーバーである。

【００１５】

ノードの内部構成の典型例を図３に示す。

【００１６】

ノードには、ルーターとホストがあり、ルーターは自分宛ではないパケットを転送するがホストは転送しない。図３からわかるように、ノード３００は、ネットワーク・インターフェイス３０１、３０２、ＣＰＵ３０３、ＲＯＭ３０４、ＲＡＭ３０５、ＨＤ（ハードディスク）３０６、電源３０７、キーボード／ポインティングデバイスのインターフェイス３０８、モニターのインターフェイス３０９、バス３１０等を有する計算機である。

【００１７】

ルーターは複数のインターフェイス３０１、３０２を持つのに対し、ホストは多くの場合は一つのインターフェイス３０１を持つ。ネットワーク・インターフェイス３０１は、リンク２０７に接続され、リンク２０７に接続された他のノードと通信する。

【００１８】

ホスト２０４、２０５、２０６は、ネットワーク・インターフェイス３０１により、リンク２０７を介して、リンク２０７に接続された他のノード、あるいは、更に、ゲートウェイ２０２を介して、インターネット２０１上のサイトと通信する。ゲートウェイ２０２（ルーター）においては、ネットワーク・インターフェイス３０１は、リンク２０７に接続され、それを介してリンク上の他の装置と通信し、ネットワーク・インターフェイス３０２はリンク２０８に接続され、それを介してインターネット２０１と接続され、それらを介してインターネット上のノードと通信する。なお、ノードによってはＨＤを持たないものもある。

【００１９】

なお以下の処理内容（手順）は、装置もしくはプログラムとして実現される。すなわち、装置で実現する形態では、その装置を有するノード３００が、以下の

処理内容（手順）を実行する。また、プログラムとして実現する形態では、そのプログラムがＲＯＭ３０４もしくはＨＤ３０６に格納されたノードが、以下の処理内容（手順）を実行する。例えば、プログラムとして実現される場合は、そのプログラムをＣＰＵ３０３が読み込み、必要に応じてＲＡＭ３０５を計算のための空間として利用しながらバス３１０を介してインターフェイス３０１、３０２にアドレスを割当てる、というような動作を行なう。

【００２０】

本実施の形態のイーサネット（Ｒ）ＬＡＮ環境で各ホストがＩＰｖ６グローバルアドレスのプレフィックスやｄｅｆａｕｌｔ　ｇａｔｅｗａｙのアドレスを取得するプロトコルの仕組みを簡単に説明し、その次に本発明を適用した具体的な実施の形態を説明する。

【００２１】

典型的なＩＰｖ６アドレスはｐｒｅｆｉｘとｉｎｔｅｒｆａｃｅ　ＩＤからなり、ｐｒｅｆｉｘが上位６４ビット、ｉｎｔｅｒｆａｃｅ　ＩＤが下位６４ビットである。ｉｎｔｅｒｆａｃｅ　ＩＤは、イーサネット（Ｒ）・インターフェイスのＭＡＣ　ａｄｄｒｅｓｓ　４８ビットを元にして以下のように生成される。

【００２２】

イーサネット（Ｒ）のＩＥＥＥ　ｉｄｅｎｔｉｆｉｅｒ（ＭＡＣ　ａｄｄｒｅｓｓ）は、６バイト長のアドレスで、先頭の３バイトは製造ベンダーコードとしてＩＥＥＥによって管理・割当てがされている。残り３バイトは各ベンダーに管理が任されており、重複が起こらないように割当てがされる。図４にイーサネット（Ｒ）のＭＡＣ　ａｄｄｒｅｓｓの構成を示す。各四角は１バイト（８ビット）のデータを示し、左から３バイトは製造ベンダーコード、残り３バイトはベンダーが管理するコードとなっている。ベンダーが管理するコードはイーサネット（Ｒ）・カード毎に異なるように振られるので、イーサネット（Ｒ）・カード毎に世界で唯一のアドレスが対応し、イーサネット（Ｒ）上でのデータの送受信の際にアドレスとして利用される。

【００２３】

イーサネット（Ｒ）のＭＡＣ　ａｄｄｒｅｓｓ（図４参照）を３バイトずつに

分割し、中間に１６進数の「ＦＦＦＥ」をはさみ、先頭から７ビット目を１にする。これを図５に示す。図５のＣ１’は、図４のＣ１の先頭から７ビット目を１にしたものを表す。このようにして生成された、図５の構成の６４ビット・データをＩＥＥＥ　ＥＵＩ－６４形式のｉｎｔｅｒｆａｃｅ　ＩＤと呼ぶ。ＩＥＥＥ　ＥＵＩ－６４形式のｉｎｔｅｒｆａｃｅ　ＩＤから生成されたＩＰｖ６アドレスをＩＥＥＥ　ＥＵＩ－６４形式のＩＰｖ６アドレスと呼ぶ。

【００２４】

次に、図３のノードが、電源を入れられたあるいはリブートされた場合に行なう動作のフローチャートを図８に示す。この動作はＤＡＤ（Duplicate Address Detection）と呼ばれる。以下では図８の流れに沿って処理内容を説明する。

【００２５】

ステップＳ８０１でノード３００が電源を入れられたあるいはリブートされた後、まずネットワーク・インターフェイス３０１のイーサネット（Ｒ）のＭＡＣ　ａｄｄｒｅｓｓ（図４参照）からｉｎｔｅｒｆａｃｅ　ＩＤ（図５参照）を作成し、それをｔｅｎｔａｔｉｖｅ　ｌｉｎｋ－ｌｏｃａｌ　ａｄｄｒｅｓｓ（図６参照）とする（ステップＳ８０２）。

【００２６】

次に、そのｔｅｎｔａｔｉｖｅ　ｌｉｎｋ－ｌｏｃａｌ　ａｄｄｒｅｓｓがリンク２０７上で一意かどうかを判断するために、ノード３００は以下の処理を行なう。

【００２７】

最初に、インターフェイス３０１の初期設定をする。すなわち、インターフェイス３０１に、ａｌｌ－ｎｏｄｅｓ　ｍｕｌｔｉｃａｓｔ　ａｄｄｒｅｓｓ（ＦＦ０２：：１）とそのｔｅｎｔａｔｉｖｅ　ｌｉｎｋ－ｌｏｃａｌ　ａｄｄｒｅｓｓのｓｏｌｉｃｉｔｅｄ－ｎｏｄｅ　ｍｕｌｔｉｃａｓｔ　ａｄｄｒｅｓｓを割当てる（図７参照）。つまり、そのインターフェイス３０１がａｌｌ－ｎｏｄｅｓ　ｍｕｌｔｉｃａｓｔ　ａｄｄｒｅｓｓ宛のパケットあるいはそのｔｅｎｔａｔｉｖｅ　ｌｉｎｋ－ｌｏｃａｌ　ａｄｄｒｅｓｓのｓｏｌｉｃｉｔｅｄ－ｎｏｄｅ　ｍｕｌｔｉｃａｓｔ　ａｄｄｒｅｓｓ宛のパケットを見つけたときはそ

れを自分のインターフェイス宛のパケットとして受け取る。

【００２８】

前者（ａｌｌ－ｎｏｄｅｓ　ｍｕｌｔｉｃａｓｔ　ａｄｄｒｅｓｓ）を割当てることによって、既にそのｔｅｎｔａｔｉｖｅ　ｌｉｎｋ－ｌｏｃａｌ　ａｄｄｒｅｓｓを使っている他のノードからのデータを受信することが可能になる。また、後者（そのｔｅｎｔａｔｉｖｅ　ｌｉｎｋ－ｌｏｃａｌ　ａｄｄｒｅｓｓのｓｏｌｉｃｉｔｅｄ－ｎｏｄｅ　ｍｕｌｔｉｃａｓｔ　ａｄｄｒｅｓｓ）を割当てることによって、同じｔｅｎｔａｔｉｖｅ　ｌｉｎｋ－ｌｏｃａｌ　ａｄｄｒｅｓｓを同時に使おうとしている他のノードの存在を検出することが可能になる。

【００２９】

あるｔｅｎｔａｔｉｖｅ　ｌｉｎｋ－ｌｏｃａｌ　ａｄｄｒｅｓｓのｓｏｌｉｃｉｔｅｄ－ｎｏｄｅ　ｍｕｌｔｉｃａｓｔ　ａｄｄｒｅｓｓとは、ＲＦＣ２４６１のｐａｇｅ９１に定義されているように、ｔｅｎｔａｔｉｖｅ　ｌｉｎｋ－ｌｏｃａｌ　ａｄｄｒｅｓｓの下位２４ビットをプレフィックスＦＦ０２：０：０：０：０：１：ＦＦ００：：／１０４に付加したデータであり、ｌｉｎｋ－ｌｏｃａｌ　ｓｃｏｐｅ　ｍｕｌｔｉｃａｓｔ　ａｄｄｒｅｓｓである。図６と図７にそれらの関係を示す。以上のアドレス割当てが図８のステップＳ８０３である。

【００３０】

次にＮｅｉｇｈｂｏｒ　Ｓｏｌｉｃｉｔａｔｉｏｎ　ｍｅｓｓａｇｅを作る。Ｎｅｉｇｈｂｏｒ　Ｓｏｌｉｃｉｔａｔｉｏｎ　ｍｅｓｓａｇｅのＴａｒｇｅｔ　Ａｄｄｒｅｓｓ（ターゲットアドレス）には判断対象のｔｅｎｔａｔｉｖｅ　ｌｉｎｋ－ｌｏｃａｌ　ａｄｄｒｅｓｓを、ＩＰ　Ｓｏｕｒｃｅ（送信元アドレス）にはｕｎｓｐｅｃｉｆｉｅｄ　ａｄｄｒｅｓｓ（１２８ビット全てが０）を、ＩＰ　ｄｅｓｔｉｎａｔｉｏｎ（宛先アドレス）には判断対象のｔｅｎｔａｔｉｖｅ　ｌｉｎｋ－ｌｏｃａｌ　ａｄｄｒｅｓｓのｓｏｌｉｃｉｔｅｄ－ｎｏｄｅ　ｍｕｌｔｉｃａｓｔ　ａｄｄｒｅｓｓを設定する。

【００３１】

このＮｅｉｇｈｂｏｒ　Ｓｏｌｉｃｉｔａｔｉｏｎ　ｍｅｓｓａｇｅをＲｅｔｒａｎｓＴｉｍｅｒミリセカンド間隔でＤｕｐＡｄｄｒＤｅｔｅｃｔＴｒａｎｓｍｉｔｓ個イーサネット（Ｒ）２０７に送出する。図８のステップＳ８０４がこの処理である。

【００３２】

Ｎｅｉｇｈｂｏｒ　Ｓｏｌｉｃｉｔａｔｉｏｎ　ｍｅｓｓａｇｅを受け取ったノードは、その送信元アドレスが　ｕｎｓｐｅｃｉｆｉｅｄ　ａｄｄｒｅｓｓならば、そのｍｅｓｓａｇｅがＤＡＤを行っているノードからのデータであることと判断する。

【００３３】

同時に複数のノードが同じアドレスを対象としてＤＡＤをしている場合は、自分が送ったＮｅｉｇｈｂｏｒ　Ｓｏｌｉｃｉｔａｔｉｏｎ　ｍｅｓｓａｇｅｓ以外にも、同じアドレスをＴａｒｇｅｔ　Ａｄｄｒｅｓｓに含むＮｅｉｇｈｂｏｒ　Ｓｏｌｉｃｉｔａｔｉｏｎ　ｍｅｓｓａｇｅｓを受け取る（自分が送ったＮｅｉｇｈｂｏｒ　Ｓｏｌｉｃｉｔａｔｉｏｎ　ｍｅｓｓａｇｅと、同時にそのアドレスを対象としてＤＡＤをしている他のノードが送ったＮｅｉｇｈｂｏｒ　Ｓｏｌｉｃｉｔａｔｉｏｎ　ｍｅｓｓａｇｅを受け取る）ので、重複していることがわかる。その場合にはどのノードもそのアドレスは使わない。

【００３４】

なお、受け取ったＮｅｉｇｈｂｏｒ　Ｓｏｌｉｃｉｔａｔｉｏｎ　ｍｅｓｓａｇｅが、自分が送ったもの（マルチキャストのパケットをループバックしているため）であるならば、他にそれを使っているあるいは使おうとしているノードが存在することを示さない。自分が送ったＮｅｉｇｈｂｏｒ　Ｓｏｌｉｃｉｔａｔｉｏｎ　ｍｅｓｓａｇｅに加えて、同じアドレスをＴａｒｇｅｔ　Ａｄｄｒｅｓｓに含むＮｅｉｇｈｂｏｒ　Ｓｏｌｉｃｉｔａｔｉｏｎ　ｍｅｓｓａｇｅｓを受け取った場合に、同時に複数のノードが同じアドレスを対象としてＤＡＤをしていると判断する。

【００３５】

一方、Ｎｅｉｇｈｂｏｒ　Ｓｏｌｉｃｉｔａｔｉｏｎ　ｍｅｓｓａｇｅを受け

取ったノードが、そのｍｅｓｓａｇｅのＴａｒｇｅｔ　Ａｄｄｒｅｓｓ（ターゲットアドレス）に含まれるアドレスを既に使っていれば、Ｔａｒｇｅｔ　Ａｄｄｒｅｓｓにそのｔｅｎｔａｔｉｖｅ　ｌｉｎｋ－ｌｏｃａｌ　ａｄｄｒｅｓｓが設定されたａ　ｍｕｌｔｉｃａｓｔ　Ｎｅｉｇｈｂｏｒ　Ａｄｖｅｒｔｉｓｅｍｅｎｔをａｌｌ－ｎｏｄｅｓ　ｍｕｌｔｉｃａｓｔ　ａｄｄｒｅｓｓ宛てに返す。従って、Ｎｅｉｇｈｂｏｒ　Ｓｏｌｉｃｉｔａｔｉｏｎ　ｍｅｓｓａｇｅを送ったノードがａｌｌ－ｎｏｄｅｓ　ｍｕｌｔｉｃａｓｔ　ａｄｄｒｅｓｓ宛てのａ　ｍｕｌｔｉｃａｓｔ　Ｎｅｉｇｈｂｏｒ　Ａｄｖｅｒｔｉｓｅｍｅｎｔを受け取り、そのｔａｒｇｅｔ　ａｄｄｒｅｓｓが（判断対象の）ｔｅｎｔａｔｉｖｅ　ａｄｄｒｅｓｓである場合（図８のＳ８０５ステップの「はい」の場合）は判断対象のｔｅｎｔａｔｉｖｅ　ａｄｄｒｅｓｓが唯一ではない（つまり、重複している）。

【００３６】

以上のＤＡＤの結果、判断対象のｔｅｎｔａｔｉｖｅ　ｌｉｎｋ－ｌｏｃａｌ　ａｄｄｒｅｓｓがリンク２０７上で唯一であることが確認された（図８のＳ８０５ステップの「いいえ」の場合）ならば、そのアドレスをリンクローカルアドレスとしてインターフェイス３０１に割当てる。これが図８のステップＳ８０６である。以上でＤＡＤは終了する。

【００３７】

以上に説明した図８の動作は図２のｇａｔｅｗａｙ　２０２、ＤＨＣＰ　ｓｅｒｖｅｒ２０３、ホスト２０４、ホスト２０５、ホスト２０６のそれぞれが実行することができる。

【００３８】

図２のホスト、例えばホスト２０６は、リンクローカルアドレスをインターフェイス３０１に割当てたら、次はサイトローカルアドレスやグローバルアドレスを決定するために必要な情報（Ｒｏｕｔｅｒ　Ａｄｖｅｒｔｉｓｅｍｅｎｔと呼ばれる）を入手することを試みる。

【００３９】

この動作を図９に示す。ｇａｔｅｗａｙ２０２が、Ｒｏｕｔｅｒ　Ａｄｖｅｒ

ｔｉｓｅｍｅｎｔを送る場合を説明する。ｇａｔｅｗａｙ２０２は通常はルーターと呼ばれるので以下ではルーター２０２と記す。ルーター２０２は管理者によって必要な設定が行われ、Ｒｏｕｔｅｒ　Ａｄｖｅｒｔｉｓｅｍｅｎｔを定期的にリンク２０７に送っている。ホスト２０６がＲｏｕｔｅｒ　Ａｄｖｅｒｔｉｓｅｍｅｎｔを早く入手したい場合は、ホスト２０６はＲｏｕｔｅｒ　Ｓｏｌｉｃｉｔａｔｉｏｎと呼ばれるデータをルーター２０２に送る。ホスト２０６はリンクローカルアドレスを割当てた直後にはルーター２０２の存在はわからないので、実際にはＲｏｕｔｅｒ　Ｓｏｌｉｃｉｔａｔｉｏｎはリンク上のルーター全てに対するマルチキャストとして送られる。図９のステップＳ９０１はこの処理を示す。

【００４０】

Ｒｏｕｔｅｒ　Ｓｏｌｉｃｉｔａｔｉｏｎを受け取ったルーター２０２はＲｏｕｔｅｒ　Ａｄｖｅｒｔｉｓｅｍｅｎｔを送る。図９のステップＳ９０２の「はい」の場合に示すように、Ｓｔａｔｅｌｅｓｓ　ａｄｄｒｅｓｓ　ａｕｔｏｃｏｎｆｉｇｕｒａｔｉｏｎのみを指定するＲｏｕｔｅｒ　Ａｄｖｅｒｔｉｓｅｍｅｎｔを受け取ったホスト２０６は、そのメッセージに含まれるプレフィックスの有効性（既にその装置によって使われていないこと等）を確認し、それ（ら）にインターフェイスＩＤを付加して作ったアドレスを、サイトローカルアドレスあるいはグローバルアドレスとし、インターフェイス３０１に割当てる。図９のステップＳ９０３がこの処理である。

【００４１】

図９のステップＳ９０２の「いいえ」の場合に示すように、ホスト２０６がｓｔａｔｅｌｅｓｓ　ａｄｄｒｅｓｓ　ａｕｔｏｃｏｎｆｉｇｕｒａｔｉｏｎのみを指定するＲｏｕｔｅｒ　Ａｄｖｅｒｔｉｓｅｍｅｎｔを受け取らなかった場合は、次の二つの場合に分けられる。Ｓｔａｔｅｌｅｓｓ　ａｄｄｒｅｓｓ　ａｕｔｏｃｏｎｆｉｇｕｒａｔｉｏｎとｓｔａｔｅｆｕｌ　ａｄｄｒｅｓｓ　ａｕｔｏｃｏｎｆｉｇｕｒａｔｉｏｎの両方を指定するＲｏｕｔｅｒ　Ａｄｖｅｒｔｉｓｅｍｅｎｔを受け取った場合（ステップＳ９０４のはいの場合）と、Ｒｏｕｔｅｒ　Ａｄｖｅｒｔｉｓｅｍｅｎｔを何も受け取らなかった場合（ステップＳ９

０４のいいえの場合）である。

【００４２】

後者の場合はｓｔａｔｅｆｕｌ　ａｄｄｒｅｓｓ　ａｕｔｏｃｏｎｆｉｇｕｒａｔｉｏｎ、すなわちＤＨＣＰｖ６のみを実行する。これがステップＳ９０６であり、その基本的な動作フローチャートを図１０に示す。

【００４３】

なお、ｓｔａｔｅｆｕｌ　ａｄｄｒｅｓｓ　ａｕｔｏｃｏｎｆｉｇｔａｔｉｏｎにおいてやり取りされるメッセージの内容や形式等の詳細は、“ｄｒａｆｔ－ｉｅｔｆ－ｄｈｃ－ｄｈｃｐｖ６－２３．ｔｘｔ”もしくはその改訂版に説明されている。以下では図１０の番号に沿って基本的な動作の流れを説明する。

【００４４】

ＤＨＣＰサーバー２０３は管理者によって必要な設定が行われている。具体的には、ノードとして自分のリンクローカルアドレスをインターフェイス３０１に割当ててあり、ＤＨＣＰサーバーとして振る舞うために必要なサイトローカルアドレスもしくはグローバルアドレスのためのプレフィックス等が設定されている。

【００４５】

図１０のステップＳ１００１で、ホスト２０４は、ＤＨＣＰサーバーにＤＨＣＰ　Ｓｏｌｉｃｉｔ　Ｍｅｓｓａｇｅを送る。ホスト２０６はどこにＤＨＣＰサーバーが存在するのかわからないので、ＤＨＣＰサーバーに対するマルチキャストとしてリンク２０７に送出する。ホスト２０６の接続されているリンク２０７とは異なるリンク（図示せず）にＤＨＣＰサーバーがいる場合には、ＤＨＣＰ　Ｓｏｌｉｃｉｔ　Ｍｅｓｓａｇｅは、実際にはＤＨＣＰリレー（図示せず）によって中継されてＤＨＣＰサーバー２０３に届く。

【００４６】

ＤＨＣＰ　Ｓｏｌｉｃｉｔ　Ｍｅｓｓａｇｅを受け取ったＤＨＣＰサーバー２０３はそれに対する返答としてＤＨＣＰ　Ａｄｖｅｒｔｉｓｅ　Ｍｅｓｓａｇｅをホスト２０６に返す。これは（別リンクの場合はＤＨＣＰリレーによって中継されて）ホスト２０６に届く。これがステップＳ１００２である。この時点でホ

スト２０６はＤＨＣＰサーバー２０３のアドレスがわかる。

【００４７】

次にステップＳ１００３でホスト２０６はＤＨＣＰ　Ｒｅｑｕｅｓｔ　Ｍｅｓｓａｇｅ　ＤＨＣＰサーバー２０３に送る。ＤＨＣＰサーバー２０３はＤＨＣＰ　Ｒｅｑｕｅｓｔ　Ｍｅｓｓａｇｅを受け取ると、ステップＳ１００４でＤＨＣＰ　Ｒｅｐｌｙ　Ｍｅｓｓａｇｅをホスト２０６に送る。

【００４８】

ステップＳ１００４でＤＨＣＰ　Ｒｅｐｌｙ　Ｍｅｓｓａｇｅ受け取ったホスト２０６は、それからサイトローカルアドレスもしくはグローバルアドレスがわかるので、そのアドレスの中のｉｎｔｅｒｆａｃｅ　ＩＤが重複しているか否かを確認するために、ＤＡＤ処理に必要な処理を行なう。つまり、インターフェイス３０１に前述のマルチキャストアドレス等を設定する。これがステップＳ１００５である。

【００４９】

次に、ステップＳ１００６でＮｅｉｇｈｂｏｒ　Ｓｏｌｉｃｉｔａｔｉｏｎ　Ｍｅｓｓａｇｅを送り、Ｎｅｉｇｈｂｏｒ　Ａｄｖｅｒｔｉｓｅｍｅｎｔ　Ｍｅｓｓａｇｅを受け取るかどうかをステップＳ１００７で判断する。受け取った場合はそのアドレスが重複しているので、別のアドレスをＤＨＣＰサーバー２０３から受け取るためにステップＳ１００３に戻り、同じ処理を繰り返す。

【００５０】

ホスト２０６は、図１０のステップＳ１００７でＮｅｉｇｈｂｏｒ　Ａｄｖｅｒｔｉｓｅｍｅｎｔ　Ｍｅｓｓａｇｅを受け取らなかった場合はそのアドレスは重複していないので、ステップＳ１００８でそのアドレスをインターフェイス３０１に割当てる。

【００５１】

以上で図９のステップＳ９０６が終わる。ステップＳ９０４でＲｏｕｔｅｒ　Ａｄｖｅｒｔｉｓｅｍｅｎｔを何も受け取らなかった場合はこれで正常終了する。

【００５２】

ステップＳ９０２でｓｔａｔｅｌｅｓｓ　ａｄｄｒｅｓｓ　ａｕｔｏｃｏｎｆｉｇｕｒａｔｉｏｎとｓｔａｔｅｆｕｌ　ａｄｄｒｅｓｓ　ａｕｔｏｃｏｎｆｉｇｕｒａｔｉｏｎの両方を指定するＲｏｕｔｅｒ　Ａｄｖｅｒｔｉｓｅｍｅｎｔを受け取った場合は、ステップＳ９０５でｓｔａｔｅｌｅｓｓ　ａｄｄｒｅｓｓ　ａｕｔｏｃｏｎｆｉｇｕｒａｔｉｏｎとｓｔａｔｅｆｕｌ　ａｄｄｒｅｓｓ　ａｕｔｏｃｏｎｆｉｇｕｒａｔｉｏｎの両方を行なう。処理内容はステップＳ９０３とＳ９０６と同じである。

【００５３】

以上のようにして、イーサネット（Ｒ）をインターフェイスとして持つホスト２０６はｓｔａｔｅｌｅｓｓ　ａｄｄｒｅｓｓ　ａｕｔｏｃｏｎｆｉｇｕｒａｔｉｏｎとｓｔａｔｅｆｕｌ　ａｄｄｒｅｓｓ　ａｕｔｏｃｏｎｆｉｇｕｒａｔｉｏｎ（ＤＨＣＰｖ６）を任意の組み合わせで適用して、リンクローカルアドレス、サイトローカルアドレス、グローバルアドレス、ｄｅｆａｕｌｔ　ｇａｔｅｗａｙ等を自動設定することができる。

【００５４】

匿名アドレスを使う場合は、以上のプロトコルが次のように拡張される。図９のステップＳ９０３あるいはステップＳ９０５において、ホスト２０６はＲｏｕｔｅｒ　Ａｄｖｅｒｔｉｓｅｍｅｎｔを受け取り、それに含まれるプレフィックスの有効性（既にその装置によって使われていないこと等）を確認し、それ（ら）にインターフェイスＩＤを付加して作ったアドレスを、サイトローカルアドレスあるいはグローバルアドレスとし、インターフェイス３０１に割当てる。この際に、ＩＥＥＥ　ＥＵＩ－６４形式で生成したｉｎｔｅｒｆａｃｅＩＤのみではなく、ランダムなｉｎｔｅｒｆａｃｅＩＤにも同じ処理を行なう。ランダムなｉｎｔｅｒｆａｃｅＩＤの生成方法は後述する。

【００５５】

新しい匿名アドレスはプレフィックスにランダムなｉｎｔｅｒｆａｃｅＩＤを付加して作られる。ホスト２０６が既にインターフェイスに割当てているアドレスと新しい匿名アドレスが同じ場合は、新しいランダムなｉｎｔｅｒｆａｃｅＩＤを生成し、新しい匿名アドレスを生成する。

【００５６】

次に、ホスト２０６は匿名アドレスを対象にＤＡＤを実行する。ＤＡＤによって、他の装置がその匿名アドレスを既に使用していることがわかった場合は、新しい匿名アドレスを生成する。最大５回まで繰り返し、その結果一意の匿名アドレスを得ることが出来ない場合は、ホスト２０６はシステム・エラーをログ（記録）に残し、匿名アドレスを生成することをあきらめる。

【００５７】

ランダムなｉｎｔｅｒｆａｃｅＩＤは、ＭＤ５ｍｅｓｓａｇｅ　ｄｉｇｅｓｔを使って生成される。ＭＤ５とは任意の入力から、ランダムな１２８ビットを出力する関数である。ＲＦＣ３０４１の方法では１２８ビットが入力される。この入力１２８ビットは上位６４ビットと下位６４ビットから次のように構成される。ｉｎｔｅｒｆａｃｅ　ＩＤを上位６４ビットとする。何らかの方法で生成したランダムな値６４ビットあるいは前回のＭＤ５の計算結果の下位６４ビットを、入力１２８ビットの下位６４ビットとする。この１２８ビットを入力としてＭＤ５ｍｅｓｓａｇｅ　ｄｉｇｅｓｔを計算し、その計算結果１２８ビットの上位６４ビットを取り出す。取り出した６４ビットの左から７ビット目をゼロにした６４ビットをｉｎｔｅｒｆａｃｅ　ＩＤとする。計算結果の下位６４ビットは、次回のＭＤ５の計算に用いるため、記録しておく。

【００５８】

次に本発明の実施の形態を説明する。上述した動作（プロトコル）を利用して、ＩＥＥＥ　ＥＵＩ－６４形式のアドレスを使用させないプロトコルを説明する。

【００５９】

なお、ＩＰの下層に位置するデータリンク層の通信は、イーサネット（Ｒ）の場合、イーサネット（Ｒ）・インターフェイスのＭＡＣ　ａｄｄｒｅｓｓを識別子とする放送型パケット通信である。従って、イーサネット（Ｒ）にアクセスできる装置は通信される全てのパケットを観測でき、各パケットの送信元ＭＡＣ　ａｄｄｒｅｓｓと宛先ＭＡＣ　ａｄｄｒｅｓｓを取得することができる。

【００６０】

本形態の特定アドレス使用制限装置の動作を、図１にそって説明する。例として、ホスト２０６がＩＥＥＥ　ＥＵＩ－６４形式のアドレスの使用を試みる場合を説明する。なお以下の処理内容（手順）は、装置もしくはプログラムとして実現される。プログラムとして実現する形態では、そのプログラムがＲＯＭ３０４もしくはＨＤ３０６に格納されたノードが、以下の処理内容（手順）を実行する。図１は、このプログラムの主要部を示す。

【００６１】

この場合、リンク２０７に接続されているならば、どのＩＰｖ６装置であってもホスト２０６のＭＡＣ　ａｄｄｒｅｓｓを取得できるので、ｇａｔｅｗａｙ２０２、ＤＨＣＰ　ｓｅｒｖｅｒ２０３、ホスト２０４、ホスト２０５（およびホスト２０６）のいずれも特定アドレス使用制限装置として動作可能である。

【００６２】

ＩＰｖ６装置が使用希望または使用するＩＰｖ６アドレスが匿名アドレス（ｔｅｍｐｏｒａｒｙ　ａｄｄｒｅｓｓ）であるか否かを、その装置のデータリンク層のＭＡＣアドレスからＩＥＥＥ　ＥＵＩ－６４形式で生成したアドレスと比較して判断するノードまたはルーター２０２を、装置２０６と同じサブネット２０７に設ける。ＩＥＥＥ　ＥＵＩ－６４形式のアドレスを使用希望する場合はそれが既に使用されている旨のメッセージをノードが送出して、装置にそのアドレスを使用させない。

【００６３】

すなわち、電源を入れられたあるいはリブートされたホスト２０６がＤＡＤを実行する。このＤＡＤにおいて、Ｎｅｉｇｈｂｏｒ　Ｓｏｌｉｃｉｔａｔｉｏｎ　ｍｅｓｓａｇｅを受け取った特定アドレス使用制限装置は、ステップＳ１０１で、そのＴａｒｇｅｔ　Ａｄｄｒｅｓｓを取り出し、それが自身のアドレスと一致するか否かを判断し、一致する場合はステップＳ１０７に、一致しない場合はステップＳ１０２に進む。

【００６４】

ステップＳ１０２で、Ｔａｒｇｅｔ　Ａｄｄｒｅｓｓの下位６４ビット（ｉｎｔｅｒｆａｃｅＩＤ）を取り出す。

【００６５】

ステップＳ１０３で、取り出したｉｎｔｅｒｆａｃｅＩＤの左から２５～４０ビットが０ｘＦＦＦＥであるか否かを判断し、０ｘＦＦＦＥでない場合は処理を終了し、０ｘＦＦＦＥである場合はステップＳ１０４に進む。

【００６６】

ステップＳ１０４で、取り出したｉｎｔｅｒｆａｃｅＩＤの左から７ビット目が１であるか否かを判断し、１でない場合は処理を終了し、１の場合はステップＳ１０５に進む。

【００６７】

ステップＳ１０５で、Ｎｅｉｇｈｂｏｒ　Ｓｏｌｉｃｉｔａｔｉｏｎ　ｍｅｓｓａｇｅを含むイーサネット（Ｒ）・パケットの送信元ＭＡＣ　ａｄｄｒｅｓｓ（送信元のデータリンク層の識別子であり、送信元の装置固有の識別子である）を取り出す。

【００６８】

ステップＳ１０６で、送信元ＭＡＣ　ａｄｄｒｅｓｓ（送信元の装置固有の識別子）からＩＥＥＥ　ＥＵＩ－６４形式で生成した６４ビットデータと、ステップＳ１０２で取り出したｉｎｔｅｒｆａｃｅＩＤとが一致するか否かを判断する。一致する場合はステップＳ１０７に進み、一致しない場合は終了する。

【００６９】

ステップＳ１０７でＩＰｖ６のＮｅｉｇｈｂｏｒ　Ｄｉｓｃｏｖｅｒｙ　Ｐｒｏｔｏｃｏｌのａ　ｍｕｌｔｉｃａｓｔ　Ｎｅｉｇｈｂｏｒ　Ａｄｖｅｒｔｉｓｅｍｅｎｔを送る。

【００７０】

以上の処理が行なわれると、ホスト２０６がＩＥＥＥ　ＥＵＩ－６４形式のｉｎｔｅｒｆａｃｅＩＤとは異なるｉｎｔｅｒｆａｃｅ　ＩＤを使おうとするときはａ　ｍｕｌｔｉｃａｓｔ　Ｎｅｉｇｈｂｏｒ　Ａｄｖｅｒｔｉｓｅｍｅｎｔを受け取らないので、それから生成されるＩＰｖ６アドレスを使える。

【００７１】

一方、ＩＥＥＥ　ＥＵＩ－６４形式のｉｎｔｅｒｆａｃｅＩＤを使おうとする

と、ａ　ｍｕｌｔｉｃａｓｔ　Ｎｅｉｇｈｂｏｒ　Ａｄｖｅｒｔｉｓｅｍｅｎｔを受け取るのでそのｉｎｔｅｒｆａｃｅＩＤおよびそれから生成されるＩＰｖ６アドレスを使えない（可能ならば、他のＩＰｖ６アドレスを生成して、用いることになる）。

【００７２】

すなわち、送信元であるホスト２０６が、送信元ＭＡＣアドレス（送信元のデータリンク層の識別子であり、送信元の装置固有の識別子である）から特定方法で生成したネットワークアドレス（ＩＥＥＥ　ＥＵＩ－６４形式のｉｎｔｅｒｆａｃｅＩＤから生成したＩＰｖ６アドレス）の使用を試みると、特定アドレス使用制限装置は、その試みを検出する。そして、そのネットワークアドレスが使用されていることを示すメッセージであるａ　ｍｕｌｔｉｃａｓｔ　Ｎｅｉｇｈｂｏｒ　Ａｄｖｅｒｔｉｓｅｍｅｎｔを送信することにより、ホスト２０６にそのネットワークアドレスの使用制限を通知する。

【００７３】

従って、プライバシを侵害される可能性をなくすことができる。

【００７４】

（第２の実施の形態）

本実施の形態では、ＩＥＥＥ　ＥＵＩ－６４形式のｉｎｔｅｒｆａｃｅＩＤから生成されたアドレスは使用されるが、それを使ってネットワーク外部とは通信させないことにより、プライバシを侵害されないようにする。

【００７５】

第１の実施の形態では、ＩＥＥＥ　ＥＵＩ－６４形式のｉｎｔｅｒｆａｃｅＩＤを一切使わせないようになっているので、他のｉｎｔｅｒｆａｃｅＩＤを生成する手段を持たないＩＰｖ６装置は、アドレスを持つことが出来ない。設定の変更をネットワーク経由でのみ行なえるＩＰｖ６装置も考えられるので、本実施の形態では、ＩＥＥＥ　ＥＵＩ－６４形式のインターフェイスＩＤから生成したリンクローカルアドレスを使えるようにし、しかし、ＩＥＥＥ　ＥＵＩ－６４形式のインターフェイスＩＤから生成したグローバルアドレスは使えないようにする特定アドレス使用制限装置を提供する。

【００７６】

本実施の形態における特定アドレス使用制限装置は、図２におけるｇａｔｅｗａｙ２０２（ルーター）として実現される。図１１にそって、その動作を説明する。なお以下の処理内容（手順）は、装置もしくはプログラムとして実現される。プログラムとして実現する形態では、そのプログラムがＲＯＭ３０４もしくはＨＤ３０６に格納されたノードが、以下の処理内容（手順）を実行する。図１１は、このプログラムの主要部を示す。特定アドレス使用制限装置は、リストを生成・管理しているものとする。このリストは、ＲＡＭ３０５に格納される。このリストには、後述のＳ１００７で、アドレスが登録される。

【００７７】

ＩＰｖ６装置が使用希望または使用するＩＰｖ６アドレスが匿名アドレス（ｔｅｍｐｏｒａｒｙ　ａｄｄｒｅｓｓ）であるか否かを、その装置のデータリンク層のＭＡＣアドレスからＩＥＥＥ　ＥＵＩ－６４形式で生成したアドレスと比較して判断するノードまたはルーター２０２を、装置と同じサブネット２０７に設ける。そのアドレスを含むパケットか否かをルーター２０２が判断して、当該パケットの場合は破棄し、ネットワーク２０７外部へ転送しない。

【００７８】

特定アドレス使用制限装置は、リンク２０７上のＩＰｖ６装置（例えば、ホスト２０６）から外部ネットワーク２０１へ転送するものとして受け取ったＩＰｖ６パケットを対象に、次の処理を行なう。外部ネットワーク２０１へ転送するものとして受け取ったＩＰｖ６パケットとは、ｄｅｓｔｉｎａｔｉｏｎ　ａｄｄｒｅｓｓが、外部ネットワーク２０１上のアドレスであるＩＰｖ６パケットである。

【００７９】

ステップＳ１００１で、対象とするＩＰｖ６パケットのｓｏｕｒｃｅ　ａｄｄｒｅｓｓを取り出し、それがリストに登録されているか否かを判定する。登録されている場合は、ステップＳ１００８に進む。登録されていない場合は、ステップＳ１００２に進む。

【００８０】

ステップＳ１００２で、対象ＩＰｖ６パケットのｓｏｕｒｃｅ　ａｄｄｒｅｓｓの下位６４ビット（インターフェイスＩＤ）を取り出す。取り出したｉｎｔｅｒｆａｃｅＩＤの左から２５～４０ビットが０ｘＦＦＦＥであるか否かを判断し、０ｘＦＦＦＥでない場合はステップＳ１００９に進み、０ｘＦＦＦＥである場合はステップＳ１００４に進む。

【００８１】

ステップＳ１００４で、取り出したｉｎｔｅｒｆａｃｅＩＤの左から７ビット目が１であるか否かを判断し、１でない場合はステップＳ１００９に進み、１の場合はステップ１００５に進む。

【００８２】

ステップ１００５で、対象のＩＰｖ６パケットを含むイーサネット（Ｒ）・パケットの送信元ＭＡＣ　ａｄｄｒｅｓｓを取り出す。

【００８３】

ステップ１００６で、送信元ＭＡＣ　ａｄｄｒｅｓｓからＩＥＥＥ　ＥＵＩ－６４形式で生成した６４ビットデータと、ステップ１００２で取り出したｉｎｔｅｒｆａｃｅＩＤとが一致するか否かを判断する。一致する場合はステップ１００７に進み、一致しない場合はステップＳ１００９に進む。

【００８４】

ステップ１００７で対象ＩＰｖ６パケットのｓｏｕｒｃｅ　ａｄｄｒｅｓｓをリストに登録し、ステップＳ１００８に進む。したがって、このアドレスがリストに登録された以降、外部ネットワークへのパケットのソースアドレス（発信元アドレス）が、このアドレスであった場合には、Ｓ１００２からＳ１００７の処理を行なうことなく、Ｓ１００１からＳ１００８へ進む。

【００８５】

ステップＳ１００８で、対象ＩＰｖ６パケットを破棄し、終了する。

【００８６】

ステップＳ１００９で、対象ＩＰｖ６パケットを外部ネットワーク２０１に転送し、終了する。

【００８７】

以上の動作から明らかなように、ＩＥＥＥ　ＥＵＩ－６４形式のｉｎｔｅｒｆａｃｅＩＤから生成されたグローバルアドレスをｓｏｕｒｃｅ　ａｄｄｒｅｓｓとするＩＰｖ６パケットは破棄されるので、外部ネットワーク２０１に転送されない。

【００８８】

一方、ＩＥＥＥ　ＥＵＩ－６４形式とは異なるインターフェイスＩＤから生成されたグローバルアドレスをｓｏｕｒｃｅ　ａｄｄｒｅｓｓとするＩＰｖ６パケットは、外部ネットワーク２０１に転送される。

【００８９】

すなわち、送信元であるホスト２０６のＭＡＣアドレス（データリンク層の識別子であり、装置固有の識別子である）から特定方法で生成したネットワークアドレス（ＩＥＥＥ　ＥＵＩ－６４形式のインターフェイスＩＤから生成したＩＰｖ６アドレス）を含むデータの送信を、特定アドレス使用制限装置が検出し、そのデータの転送を中止する。

【００９０】

従って、プライバシを侵害される可能性をなくすことができる。

【００９１】

【発明の効果】

本発明によれば、プライバシの侵害を防ぐことができる。

【００９２】

ＩＰｖ６ネットワークにおいて、特定方法、例えばＩＥＥＥ　ＥＵＩ－６４形式でｉｎｔｅｒｆａｃｅＩＤを生成する装置、あるいはＩＥＥＥ　ＥＵＩ－６４形式で生成されたｉｎｔｅｒｆａｃｅＩＤからＩＰｖ６アドレスを生成する装置が、そのｉｎｔｅｒｆａｃｅＩＤあるいはそのＩＰｖ６アドレスを使用できないようにすることができる。従って、そのＩＰｖ６アドレスを使用することによりプライバシを侵害される可能性をなくす効果が得られる。

【００９３】

これにより、ＩＥＥＥ　ＥＵＩ－６４形式で生成されたｉｎｔｅｒｆａｃｅＩＤを使用してしまうことがなくなり、ＩＰｖ６装置およびそのユーザのプライバ

シを保護できる。

【００９４】

また、プライバシが侵害される恐れがあるアドレスを用いて、ネットワーク外部とは通信できないようにすることができる。

【００９５】

ＩＥＥＥ　ＥＵＩ－６４形式のアドレスを使用することは可能だが、それを用いてネットワーク外部とは通信できないようにすることができる。

【００９６】

これにより、ＩＥＥＥ　ＥＵＩ－６４形式のアドレスを使ってネットワーク内部の通信は行なえるので、ネットワーク設定が簡便であるというＩＰｖ６がそもそも持つ特徴を維持しながら、ＩＥＥＥ　ＥＵＩ－６４形式で生成されたｉｎｔｅｒｆａｃｅＩＤを不用意に使用してしまうことはなくなるので、ＩＰｖ６装置のユーザの使い勝手を悪くせずにプライバシを保護できる。

【００９７】

対象とするＩＰｖ６装置そのものにはいかなる変更も加えないので、既存のＩＰｖ６装置を対象に上記効果を得ることができる。

【図面の簡単な説明】

【図１】

アドレス判断の動作フローチャートである。

【図２】

イーサネット（Ｒ）ＬＡＮの模式図である。

【図３】

ノードの構成図である。

【図４】

イーサネット（Ｒ）のＭＡＣ　ａｄｄｒｅｓｓの構成図である。

【図５】

ｉｎｔｅｒｆａｃｅＩＤの構成図である。

【図６】

ａ　ｔｅｎｔａｔｉｖｅ　ｌｉｎｋ－ｌｏｃａｌ　ａｄｄｒｅｓｓの構成図で

ある。

【図７】

あるｔｅｎｔａｔｉｖｅ　ｌｉｎｋ－ｌｏｃａｌ　ａｄｄｒｅｓｓのｓｏｌｉｃｉｔｅｄ－ｎｏｄｅ　ｍｕｌｔｉｃａｓｔ　ａｄｄｒｅｓｓの構成図である。

【図８】

ホストがＤＡＤを終えるまでの動作を説明するフローチャート図である。

【図９】

ホストがアドレス自動設定を終えるまでの動作を説明するフローチャート図である。

【図１０】

ホストがＤＨＣＰでアドレスを取得するまでの動作フローチャート図である。

【図１１】

転送判断の動作フローチャートである。

【符号の説明】

２０１　インターネット

２０２　ｇａｔｅｗａｙ

２０３　ＤＨＣＰサーバー

２０４　ホスト

２０５　ホスト

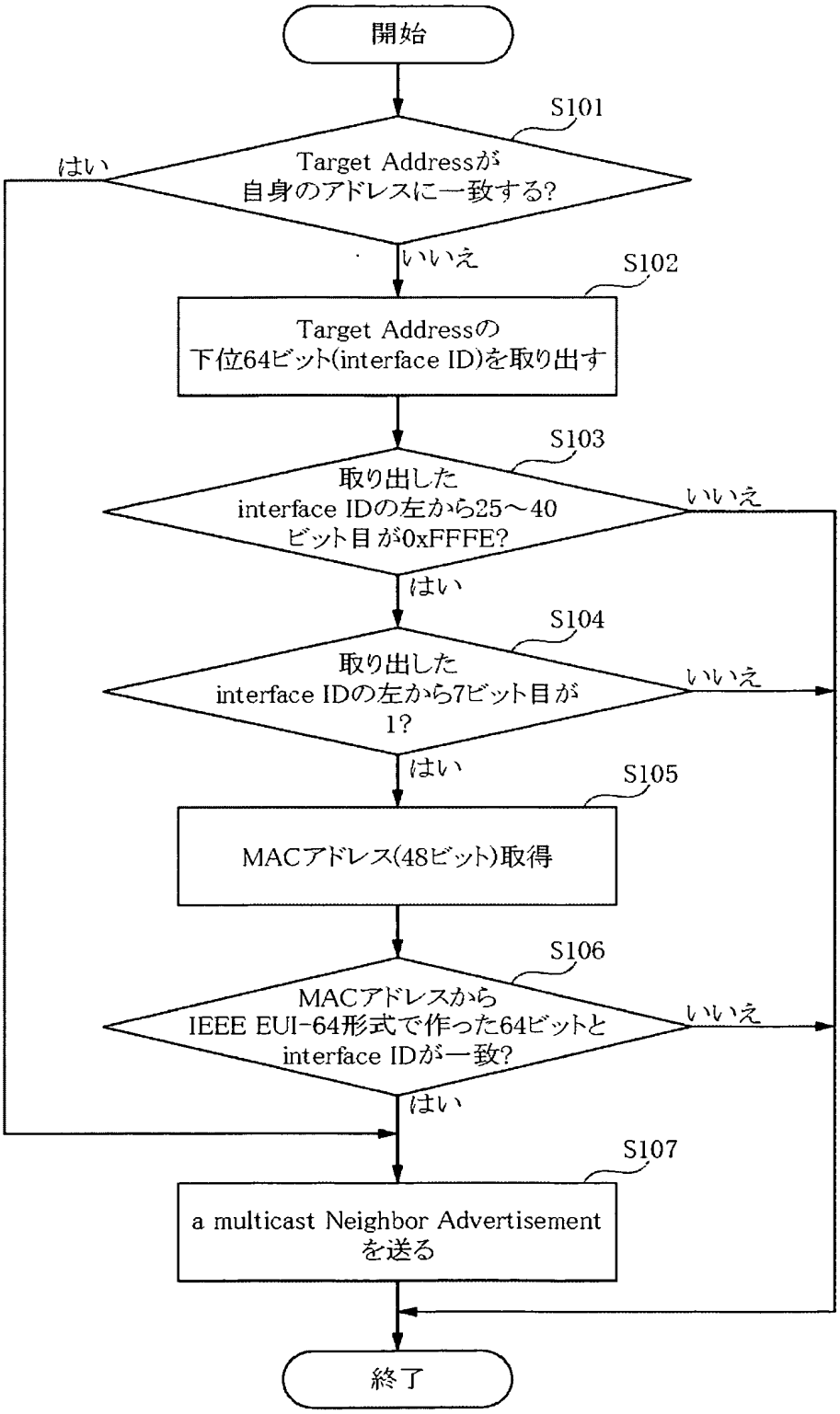
２０６　ホスト

２０７　リンク

２０８　リンク

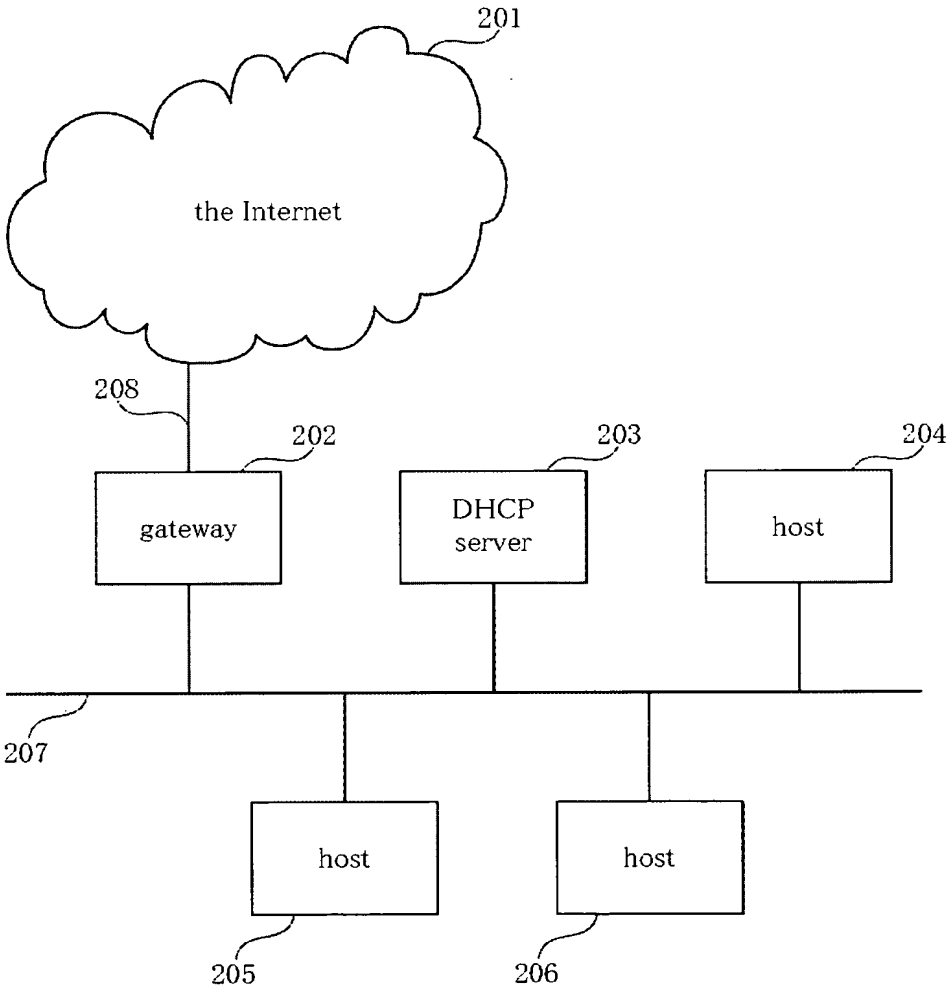
【書類名】　図面

【図１】



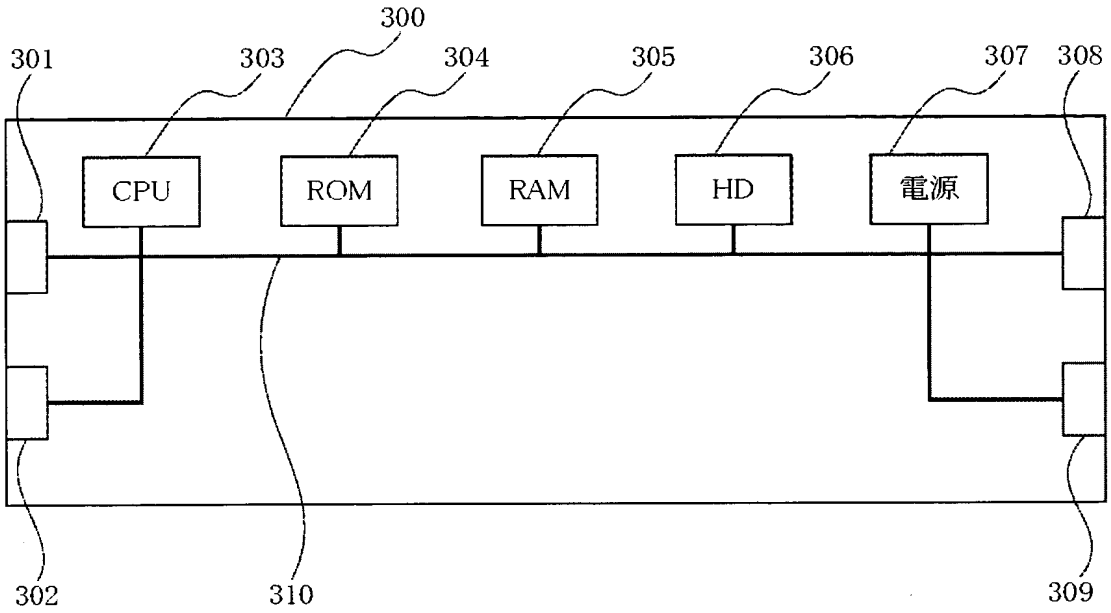
アドレス判断の動作フローチャート

【図２】



イーサネットLANの模式図

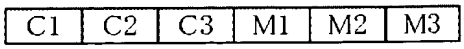
【図３】



ノードの構成

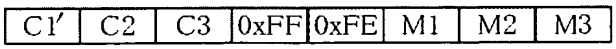
300 ノード筐体
301 ネットワーク・インターフェイス
302 ネットワーク・インターフェイス
303 CPU
304 ROM
305 RAM
306 HD(ハードディスク)
307 電源
308 キーボード/ポインティングデバイスのインターフェイス
309 モニタのインターフェイス
310 バス

【図４】



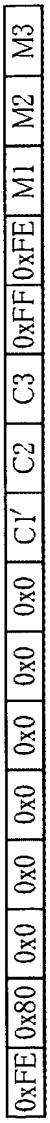
イーサネットのMACアドレスの構成

【図５】



インターフェイスIDの構成

【図６】

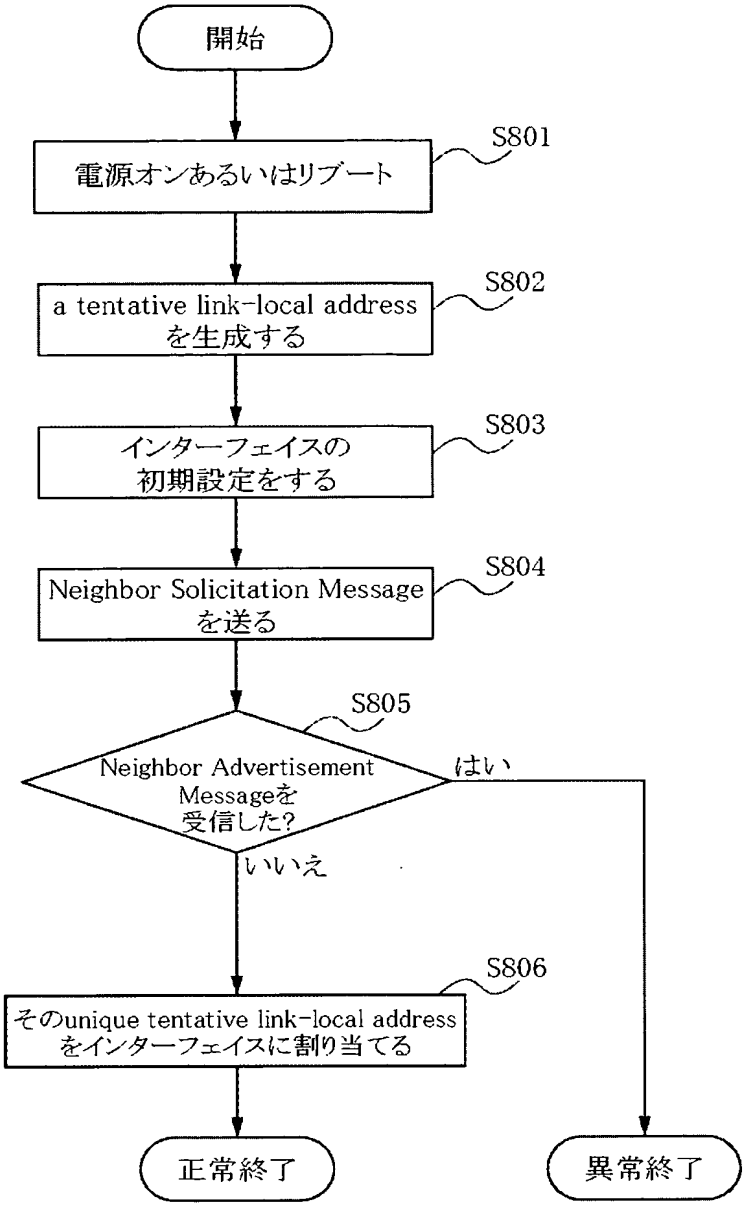


a tentative link-local addressの構成

【図７】

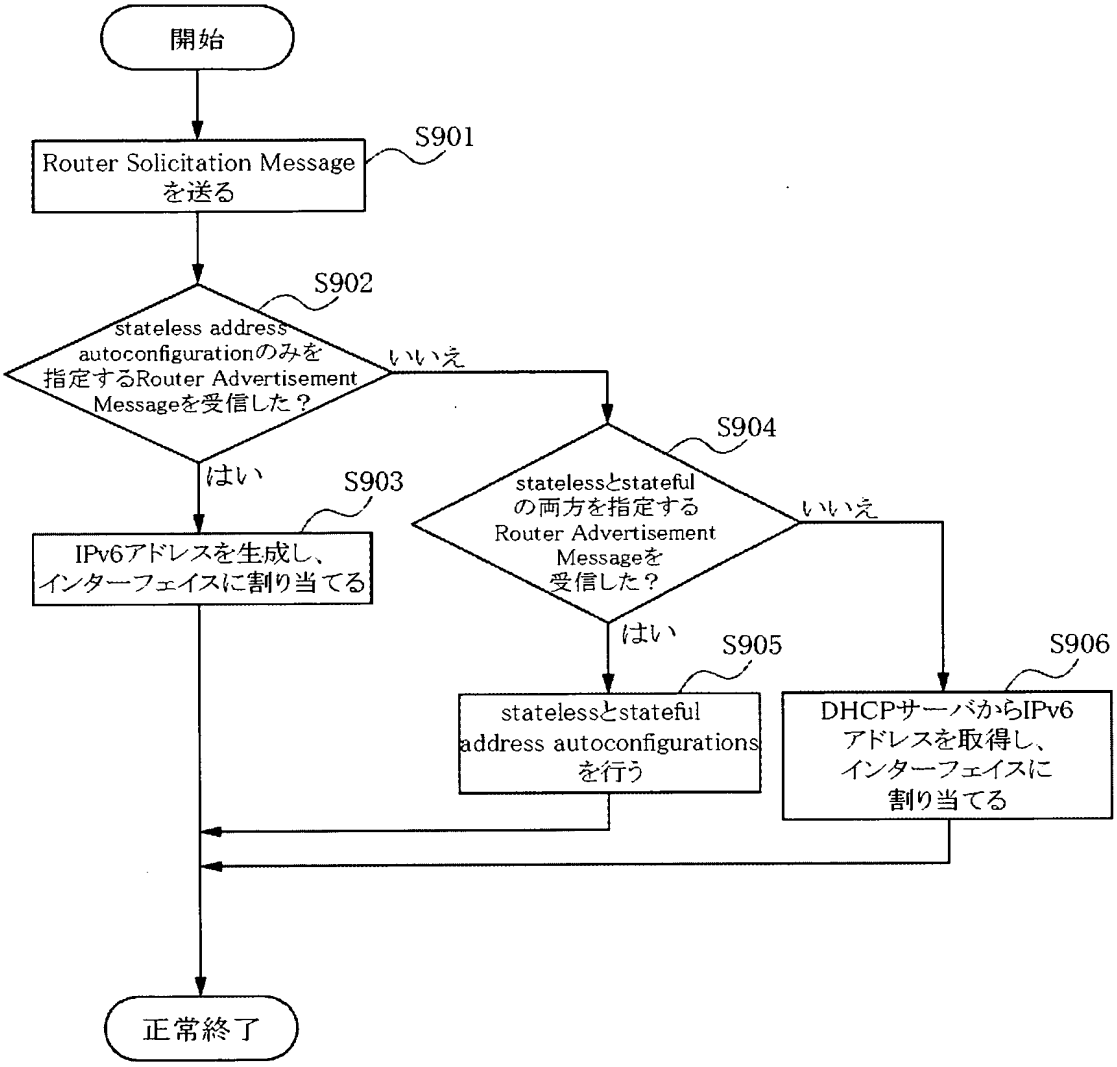
ある tentative link-local addressの solicitend-node multicast addressの構成

【図８】



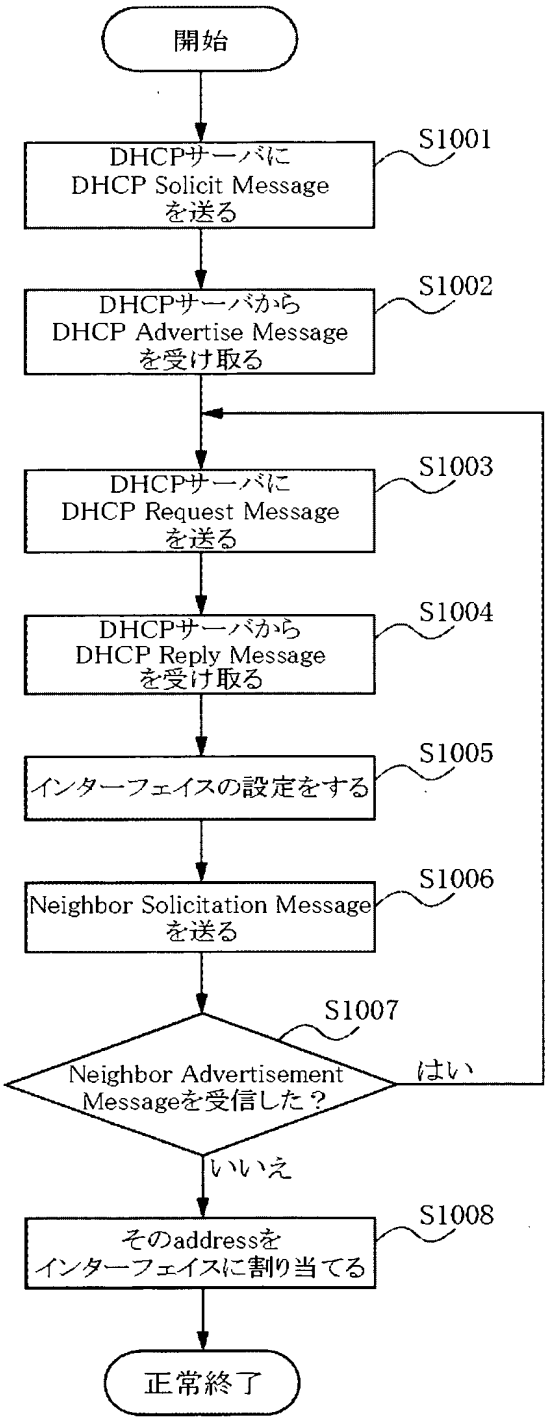
ホストがDADを終えるまでの動作フローチャート

【図９】



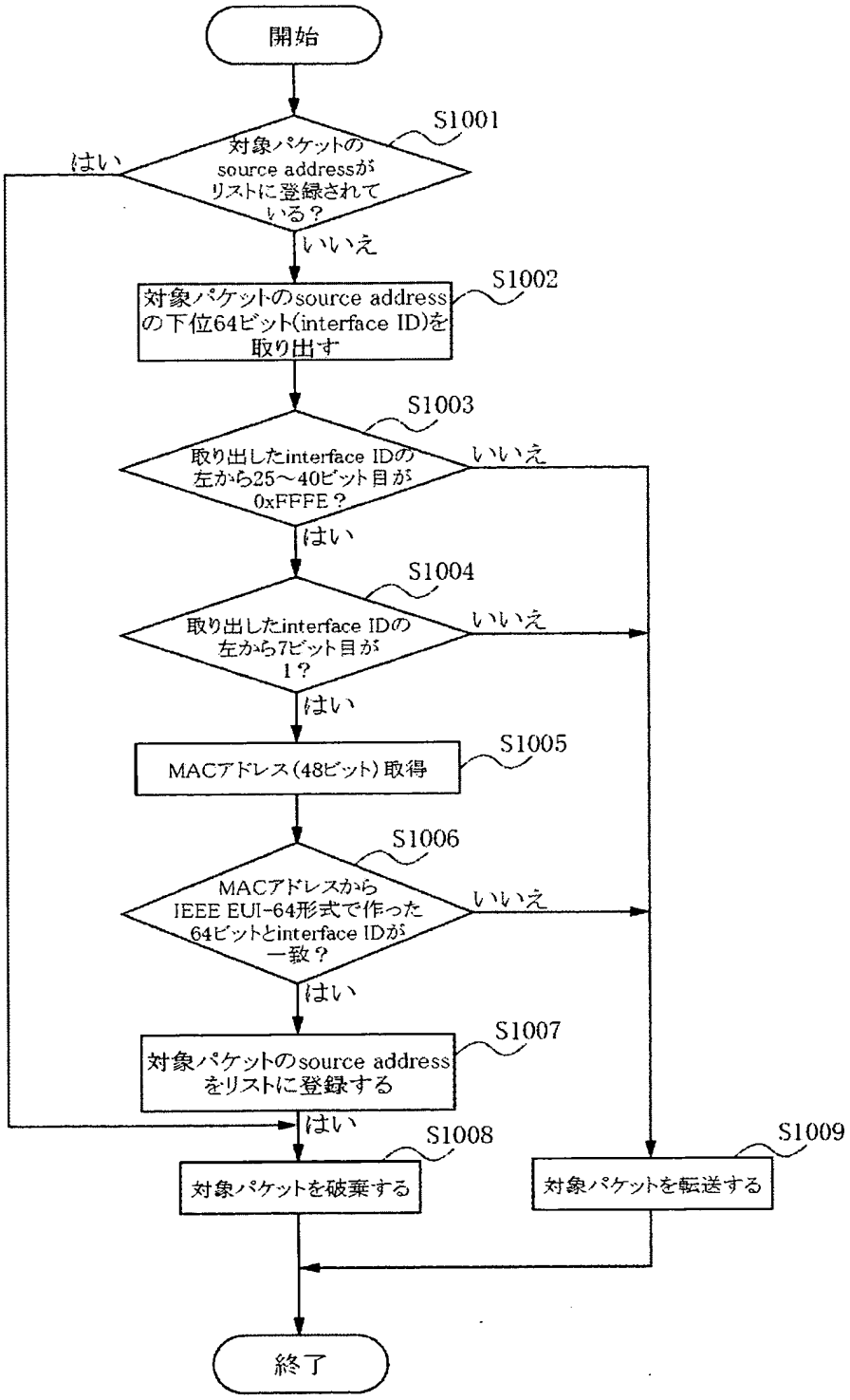
ホストがアドレス自動設定を終えるまでの動作フローチャート

【図１０】



ホストがDHCPでアドレスを取得するまでの動作フローチャート

【図１１】



転送判断の動作フローチャート

【書類名】　要約書

【要約】

【課題】　ＩＰｖ６装置が装置固有の識別情報を含むＩＥＥＥ　ＥＵＩ－６４形式のアドレスを使うと、それらの通信をモニターされてプライバシが侵害される可能性がある。

【解決手段】　ＩＰｖ６装置が使用希望または使用するＩＰｖ６アドレスが匿名アドレス（ｔｅｍｐｏｒａｒｙ　ａｄｄｒｅｓｓ）であるか否かを、その装置のデータリンク層のＭＡＣアドレスからＩＥＥＥ　ＥＵＩ－６４形式で生成したアドレスと比較して判断するノードまたはルーター２０２を、装置と同じサブネット２０７に設ける。ＩＥＥＥ　ＥＵＩ－６４形式のアドレスを使用希望する場合はそれが既に使用されている旨のメッセージをノードが送出して、装置にそのアドレスを使用させない。あるいは、そのアドレスを含むパケットか否かをルーター２０２が判断して、当該パケットの場合は破棄し、ネットワーク外部へ転送しない。

【選択図】　図２

特願２００３－１５２８３４

出　願　人　履　歴　情　報

識別番号　［０００００１００７］

１．変更年月日　１９９０年　８月３０日
［変更理由］　新規登録
住　所　東京都大田区下丸子３丁目３０番２号
氏　名　キヤノン株式会社